

REMARKS

Claims 1-16 are currently pending in the patent application. The Examiner has objected to the drawings, since Figure 1 was not labeled as Prior Art. Applicants are submitting replacement drawings and will later submit formal drawings once the change has been approved by the Examiner.

The Examiner has objected to the language of Claims 1 and 7 for reciting "a said packet". Applicants submit amendments to correct the objectionable language.

The Examiner has rejected Claims 1, 6-9, 15 and 16 for reciting "comparing the size of the data in a packet" and asks how "said first connection and said second connection are to be included in the same chain". Applicants have amended the claim language, consistent with the teachings found on page 19 of the Specification, to recite determining whether the packet at the first connection and the packet at the second connection are the same packet and whether the first and second connection are to be included in the same chain. The amendment language is adequately supported in the Specification, for example the teachings found on page 13, from lines 2-11, which state that "the logs of individual packets that are exchanged at a plurality of positions on the network along the access

JP919990248-US1

-13-

chain as the link are recorded, so that an intrusion route can be identified based on the header information in the packet and the time the information was detected". Supporting teachings for the storing of packet information are found at page 18, lines 28-page 19, lines 15 and at page 19, lines 16-25 wherein it states "[T]he size (in bytes) of the data extracted from the received packet is entered into Caplen. The actual size (length in bytes) of the packet when received by the network card is entered in Len. And the data contents (bytes)...are written in the Data portion." The comparison step is detailed from page 22, line 16 through page 23, line 6 with reference to Fig.

9. Applicants believe that the amendments are fully supported by the Specification and that the amendments address the Examiner's concerns regarding enablement. With regard to Claims 2, 9 and 16, the Examiner has reiterated the enablement concern. Applicants assert that the Specification is fully enabling and have amended the claim language with teachings from the Specification to address the Examiner concerns. The Examiner has also rejected Claims 1, 2, 5-9, 15 and 16 under 35 USC 112. Applicants believe that the amendments referenced above address the examiner's concerns and respectfully request withdrawal of the rejections.

JP919990248-US1

-14-

The Examiner has rejected Claims 1, 3-8, and 10-14 under 35 USC 102 as being anticipated by the teachings of Munger; and, has rejected Claims 2, 9, 15, and 16 under 35 USC 103 as being unpatentable over Munger in view of Aoki. For the reasons set forth below, Applicants believe that the claims are patentable over the cited art.

The present invention is directed to a system, program storage device, and method for tracing an access chain from an attacker to a target computer by identifying packets that have been routed via third party computers located between the attacker location and the target location, or an intermediate location that realizes that an attack is being launched using the packet. Routers associated with computers in a network store packet information, including such information as packet size, the length of data contents within the packet, and a time stamp, for every packet at each connection. The stored packet information is compared for different connections in order to determine if the same packet has been routed to the computers associated with those connections. Packet size and/or the length in bytes of the data in the packet comprise packet information that can readily be stored and compared to recognize packets.

JP919990248-US1

-15-

The Munger patent does not anticipate the claims of the present invention. Munger teaches a routing protocol (TARP) wherein the a router conceals the destination of a packet in the header (see: Col. 3, lines 7-11). Further, under the Munger system, nodes have more than one address (see: Col. 15, lines 16-20) that may be used to "confuse" any would-be hackers. As taught in Munger at Col. 15, lines 21-60, a router creates different "hopblocks" comprised of source address, destination address, a seed and an algorithm for packets. Successive packets get different hopblocks so that the actual destinations are concealed. Before assigning a hopblock to a packet, the router uses its randomized process to predict where the next packet will be destined and creates 5 different source/destination pairs based on its predictions. If the routing information for an incoming packet to be routed does not match one of the predicted pairs, the packet is discarded (see: Col. 15, line 61 through Col. 16, line 15). If the incoming packet to be routed does match one of the predicted pairs, then the packet is given a new hopblock in the header and is routed.

Applicants respectfully assert that the Munger patent neither teaches nor suggests the invention as claimed. The router of Munger creates random hopblocks to disguise the actual destinations of packets. There is nothing in Munger JP919990248-US1

that teaches or suggests that the router stores actual received packet information. Rather, Munger intentionally changes packet header information. Clearly, the reassigning of packet headers does not anticipate the claimed step of storing packet information and using stored packet information for tracing access chains. Further, the Munger patent teaches that an incoming packets is compared to predicted packet information. Munger does not compare actual stored packet information for a first connection to actual stored packet information for a second connection. Rather, the Munger router compares predicted destination addresses to actual destination addresses, and then either discards the packet or routes the packet after having changed the actual destination address to a randomly-generated address. Munger teaches that packet order (or sequence) must be maintained and that different sites must synchronize with each other in order to ensure packet order. Such synchronizing is done within one session, along one connection between sites. Clearly such teachings do not anticipate or obviate the comparison of packet information extracted and stored from different connections across a distributed network of computers.

JP919990248-US1

-17-

limitations thereto. With specific reference to Claim 14, which recites the recording unit, a transmitter, and a receiver, Applicants aver that the Munger patent does not teach or suggest a recording unit for recording packet data that include information concerning packet size and detection time, a transmitter for transmitting the recorded packet data to a different site for a determination regarding packet similarity and access chain, and a receiver for receiving the determination result. Accordingly, Applicants conclude that the Munger patent does not anticipate the language of Claims 1, 3-8, and 10-14.

The Examiner has additionally rejected the language of Claims 2, 9, 15 and 16 as unpatentable over Munger in view of Aoki. Applicants rely on the discussion and arguments presented above with regard to the teachings of the Munger patent. The Aoki patent is cited for the teachings found in Col. 3, lines 15-22 which provide for "adding a plurality of amounts of packet data which may possibly be sent at a present packet sending time to the amount of packet data stored in the sent data amount storage means 11 thereby to obtain a plurality of total amounts of packet data". The total is then divided by the time period for sending to calculate a data transmission rate. Aoki does not teach that a sending site store "data including at least packet JP919990248-US1

-19-

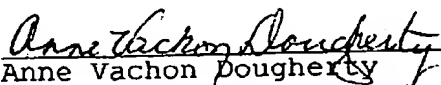
size and data length" as well as a time stamp, as is taught and claimed by the present invention. Rather, Aoki stores "an amount of packet data sent from a preset time to a preceding packet sending timing". Since Aoki is concerned with transmission rates, Aoki tracks all packet data sent within a period of time, which may encompass multiple data packets. One could not identify a particular packet based on packet length if the stored information included a total for the length of multiple packets sent over a time period. Accordingly, Applicants conclude that the Examiner erred in interpreting the Aoki teachings, and conclude that the claim language is not obviated by the combination of teachings of Munger and Aoki.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

K. Yoda, et al

By:


Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910

JP919990248-US1

-20-